

Bezpieczeństwo płatności w sieci

Jak powszechnie wiadomo świat się rozrasta. Niestety i na lepsze i na gorsze. Przez powstanie Internetu o wiele łatwiej jest nas oszukać.

Strony phishingowe, to strony tworzone przez oszustów, mające na celu wyłudzenie od nas danych wrażliwych. Strony te często są tworzone, na podobieństwo stron gigantów korporacyjnych, aby łatwiej nas oszukać.

Aby chronić się przed stronami phishingowymi:

Należy:

- Wchodzić w linki z nieznanymi źródłami;
- Podawać żadnych prywatnych danych, czy wpłacać jakichkolwiek nawet najmniejszych kwot na niezweryfikowanych stronach. Przede wszystkim nie możemy na takich stronach podawać żadnych haseł;

Nie należy:

- Sprawdzać dokładnie adres strony, ponieważ może się różnić nawet jedną literą od strony, na którą chcemy wejść.
- Sprawdzać ważność certyfikatu strony. Aby to sprawdzić wystarczy nacisnąć ikonę kłódki znajdującej się po lewej stronie paska adresu. Kłódka musi być zamknięta.
- Sprawdzić czy adres witryny zaczyna się od „https” zamiast „http”. Https oznacza bezpieczne połączenie.

Spam są to niechciane, wysyłane masowo wiadomości, często oferujące super przeceny, produkty i inne. Dużo często podają linki do tak zwanych stron tinyurl.

Strony tinyurl to strony wykradające nasz adres ip, dzięki czemu mogą uzyskać dostęp do naszego komputera, a przez komputer do naszych kont bankowych.